IT POLICY

IT Governance

IT Governance is an integral part of corporate governance. It involves leadership support, organizational structure and processes to ensure that the NBFC's IT sustains and extends business strategies and objectives. Effective IT Governance is the responsibility of the Board of Directors and Executive Management.

Well-defined roles and responsibilities of Board and Senior Management are critical, while implementing IT Governance. Clearly-defined roles enable effective project control. People, when they are aware of others' expectations from them, are able to complete work on time, within budget and to the expected level of quality. IT Governance Stakeholders include: Board of Directors, IT Strategy Committees, CEOs, Business Executives, Chief Information Officers (CIOs), Chief Technology Officers (CTOs), IT Steering Committees (operating at an executive level and focusing on priority setting, resource allocation and project tracking), Chief Risk Officer and Risk Committees.

The basic principles of value delivery, IT Risk Management, IT resource management and performance management must form the basis of governance framework. IT Governance has a continuous life-cycle. It's a process in which IT strategy drives the processes, using resources necessary to execute responsibilities. Given the criticality of the IT, NBFCs may follow relevant aspects of such prudential governance standards that have found acceptability in the finance industry.

NBFCs with asset size below ₹ 500 crore

It is recommended that smaller NBFCs may start with developing basic IT systems mainly for maintaining the database. NBFCs having asset size below ₹ 500 crore shall have a Board approved Information Technology policy/Information system policy. This policy may be designed considering the undermentioned basic standards and the same shall be put in place by September 30, 2018. The IT systems shall have:

I. Basic security aspects such as physical/ logical access controls and well defined password policy;
II. A well-defined user role;
III. A Maker-checker concept to reduce the risk of error and misuse and to ensure reliability of data/information;
IV. Information Security and Cyber Security;
V. Requirements as regards Mobile Financial Services, Social Media and Digital Signature Certificates as indicated in para 3.18, 3.10 & 3.11 above;
VI. System generated reports for Top Management summarising financial position including operating and non-operating revenues and expenses, cost benefit analysis of segments/verticals, cost of funds, etc.;
VII. Adequacy to file regulatory returns to RBI (COSMOS Returns);

VIII. A BCP policy duly approved by the Board ensuring regular oversight of the Board by way of periodic reports (at least once every year);

IX. Arrangement for backup of data with periodic testing.

X. IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases.

Purchase

1) The Admin Dept. procedures & guidelines need to be followed to purchase new technological equipment, services or software for official purposes.

2) All approved equipment, services or software will be purchased through the Admin Dept., unless informed/permitted otherwise.

3) IT Dept will assist the Admin Dept. while evaluating best and most cost-effective hardware or software to be purchased for a particular dept./project/purpose based on the requirement. The IT Dept. will also make sure all hardware/software standards defined in the IT Policy are enforced during such purchases.

4) Complete details related to purchase of technological equipment, services or software can be found in the Procurement Policy Manual.

Compliance

1) All employees are expected to comply with the IT Policy rules and guidelines while purchasing, using and maintaining any equipment or software purchased or provided by the organization.

2) Any employee who notices misuse or improper use of equipment or software within the organization must inform his/her Reporting Manager(s) immediately.

3) Inappropriate use of equipment and software by an employee will be subject to disciplinary action as deemed fit by the Management Committee of the organization.

Employee Training

1) Basic IT training and guidance is provided to all new employees about using and maintaining their Personal Computer (PC), peripheral devices and equipment in the organization, accessing the organization network and using application software.

2) Employees can request and/or the Management Committee can decide to conduct an IT training on a regular or requirement basis.

IT Support

1) SITS uses mail or tele-call System to provide IT Support to its employees and clients.

2) Employees may need hardware/software installations or may face technological issues which cannot be resolved on their own. Employees are expected to get help from the IT Dept. for such issues via telecall or Email ID – accounts@southindiancredits.com /admin@southindiancredits.com only.

3) For the sake of quick understanding, employees are expected to provide details of their issue or help required in the Ticket raised or Support Email sent.

4) For major issues like PC replacement, non-working equipment, installation of application software and more, it is mandatory for all employees to inform the IT Dept/Admin Dept.

5) For any damage to Personal Computers, approval from Reporting Manager would be required for PC replacements.

6) After raising a ticket , employees should expect a reply from the IT Dept. within 1 working day. The IT Dept. may ask the employee to deposit the problematic equipment to the IT Dept. for checking and will inform the timeline for repair/maintenance/troubleshooting/installations or the required work.

7) If there is no response in 1 working day, then the IT Dept. Designated Staff should be asked for an explanation for the delay. If no response is obtained in 3 working days, a complaint can be raised through an email to the employee's Reporting Manager and IT Dept. Designated Staff.

8) Tickets will be resolved on a First-Come-First-Served basis. However, the priority can be changed on request at the sole discretion of the designated team in IT Dept.

Equipment Purchase

1) The following equipment is purchased by the organization and provided to individual employees, departments or projects for their official use. The list can be modified as and when required. a. Personal Computing Devices (Desktop, Laptop, Tablet) b. Computer Peripherals (Printer, Scanner, Photocopier, Fax Machine, Keyboard, Mouse, Web Camera, Speaker, Modem etc.) c. Networking Equipment & Supplies (Router, Switch, Antenna, Wiring, etc.) d. Cell phones e. Biometric Devices

2) The Admin Dept. procedures & guidelines need to be followed to purchase new equipment for official purposes. All approved equipment will be purchased through the Procurement Dept., unless informed/permitted otherwise.

3) The Admin Dept. will maintain a small inventory of standard PCs, software and equipment required frequently to minimize delay in fulfilling critical orders.

Inventory Management

1) The Admin Dept. is responsible for maintaining an accurate inventory of all technological assets, software and tangible equipment purchased by the organization.

2) The following information is to be maintained for above mentioned assets in an Inventory Sheet: a. Item b. Brand/ Company Name c. Serial Number d. Basic Configuration (e.g. HP Laptop, 120 GB HD, 2 GB RAM etc.) e. Physical Location f. Date of Purchase g. Purchase Cost h. Current Person In-Charge

3) Proper information about all technological assets provided to a specific department, project or center must be regularly maintained in their respective Inventory Sheets by an assigned coordinator from that dept., project or center on a regular basis. The information thus maintained must be shared with the Procurement Dept. as and when requested.

4) When an Inventory Sheet is updated or modified, the previous version of the document should be retained. The date of modification should be mentioned in the sheet.

5) All technological assets of the organization must be physically tagged with codes for easy identification.

6) Periodic inventory audits will be carried out by the IT /Admin Dept. to validate the inventory and make sure all assets are up-to-date and in proper working condition as required for maximum efficiency and productivity.

Equipment Allocation, De-allocation & Relocation

1) Allocation of Assets: a. New Employees may be allocated a personal computer (desktop or laptop) for office work on the Day of Joining, as per work requirement. b. If required, employees can request their Reporting Manager(s) for additional equipment or supplies like external keyboard, mouse etc. c. Allocation of additional assets to an employee is at the sole discretion of the Reporting Manager(s). d. No employee is allowed to carry official electronic devices out of office without permission from Reporting Manager.

2) De-allocation of Assets:

a. It is the Reporting Manager's responsibility to collect all allocated organizational equipment & other assets from an employee who is leaving the organization. b. Updating the Inventory Sheet is mandatory after receiving back all allocated equipment. c. The received assets must be returned back to the Admin. Dept.

Equipment Usage, Maintenance and Security

1) It is the responsibility of all employees to ensure careful, safe and judicious use of the equipment & other assets allocated to and/or being used by them.

2) Proper guidelines or safety information must be obtained from designated staff in the IT /Admin Dept. before operating any equipment for the first time.

3) Any observed malfunction, error, fault or problem while operating any equipment owned by the organization or assigned to you must be immediately informed to the designated staff in IT Dept.

4) Any repeated occurrences of improper or careless use, wastage of supplies or any such offense compromising the safety or health of the equipment and people using them will be subject to disciplinary action.

5) If your assigned computing device is malfunctioning or underperforming and needs to be replaced or repaired, then written approval from your Reporting Manager is required for the same. The malfunctioning device needs to be submitted to the IT/Admin Dept. for checking, maintenance or repair. The IT /Admin Dept. staff person will give a time estimate for repair/maintenance.

6) The Reporting Manager can be informed about excessive delay or dissatisfaction about the repair or maintenance performed by the IT /Admin Dept. The issue will then be resolved by the Reporting Manager in consultation with the IT Dept. Head. The Management Committee can be consulted in terms of serious disputes or unresolved issues.

Phone Usage Policy

1) Landline phone systems are installed in the organization's offices to communicate internally with other employees and make external calls.

2) The landline phones should be strictly used to conduct official work only. As far as possible, no personal calls should be made using landline phones owned by the organization.

3) Long distance calls should be made after careful consideration since they incur significant costs to the organization.

4) The Admin. Dept. is responsible for maintaining telephone connections in offices. For any problems related to telephones, they should be contacted.

5) Employees should remember to follow telephone etiquette and be courteous while representing themselves and the organization using the organization's phone services.

Personal Computer Standards

General Guidelines

1) It is the responsibility of the IT /Admin Dept. to establish and maintain standard configurations of hardware and software for PCs owned by the organization. The standard, can however, be modified at any point in time as required by the IT /Admin Dept. Head in consultation with the Management Committee.

2) Multiple configurations are maintained as per the different requirements of various departments and projects in the organization, in consultation with the Dept./Project Head.

3) Only in exceptional cases, when none of the standard configurations satisfy the work requirements, can an employee request a non-standard PC configuration. Valid reasons need to be provided for the request and written approval of the Reporting Manager(s) is required for the same.

Network Access

1) All PCs being used in the organization are enabled to connect to the organization's Local Area Network as well as the Internet.

2) Network security is enabled in all PCs through Firewall, Web Security and Email Security software.

3) Employees are expected to undertake appropriate security measures as enlisted in the IT Policy.

Antivirus Software

1) Approved licensed antivirus software is installed on all PCs owned by the organization.

2) Two configurations – Basic and Advanced are maintained for Antivirus software installed on organization's computers. The configurations are installed on PCs as per work requirement of particular Dept./Project.

3) Employees are expected to make sure their Antivirus is updated regularly. The IT/Admin Dept. should be informed if the Antivirus expires.

4) Any external storage device like pen drive or hard disk connected to the PC needs to be completely scanned by the Antivirus software before opening it and copying files to/from the device.

Internet Usage Policy

General Guidelines

1) Internet is a paid resource and therefore shall be used only for office work.

2) The organization reserves the right to monitor, examine, block or delete any/all incoming or outgoing internet connections on the organization's network.

3) The organization has systems in place to monitor and record all Internet usage on the organization's network including each website visit, and each email sent or received. The Management Committee can choose to analyze Internet usage and publicize the data at any time to assure Internet usage is as per the IT Policy.

4) The organization has installed an Internet Firewall to assure safety and security of the organizational network. Any employee who attempts to disable, defeat or circumvent the Firewall will be subject to strict disciplinary action

Internet Login Guidelines

1) All employees may be provided with a Username and Password to login to the Internet network in the office and to monitor their individual usage.

2) An employee can also get a local static IP address for internet and intranet use. All employees will be responsible for the internet usage through this local static IP.

3) Username and password for a new employee must be requested by the HR Dept.

4) Sharing the Username and Password with another employee, visitor or guest user is prohibited. 5) A visitor or guest user who wants to use the office Internet will be given a Guest Username and Password.

6) The IT /Admin Dept. will define guidelines for issuing new passwords or allowing employees to modify their own passwords.

7) Any password security breach must be notified to the IT Dept. immediately

8) Username and password allotted to an employee will be deleted upon resignation/termination/retirement from the organization

Password Guidelines

The following password guidelines can be followed to ensure maximum password safety.

1) Select a Good Password: a. Choose a password which does not contain easily identifiable words (e.g. your username, name, phone number, house location etc.). b. Use 8 or more

characters. c. Use at least one numeric and one special character apart from letters. d. Combine multiple unrelated words to make a password.

2) Keep your Password Safe: a. Do not share your password with anyone. b. Make sure no one is observing you while you enter your password. c. As far as possible, do not write down your password. If you want to write it down, do no display it in a publicly visible area. d. Change your password periodically (every 3 months is recommended). e. Do not reuse old passwords. If that is difficult, do not repeat the last 5 passwords.

3) Other Security Measures: a. Ensure your computer is reasonably secure in your absence. b. Lock your monitor screen, log out or turn off your computer when not at desk.

Online Content Usage Guidelines

1) Employees are solely responsible for the content accessed and downloaded using Internet facility in the office. If they accidentally connect to a website containing material prohibited by the organization, they should disconnect from that site immediately.

2) During office hours, employees are expected to spend limited time to access news, social media and other websites online, unless explicitly required for office work.

3) Employees are not allowed to use Internet for non-official purposes using the Internet facility in office.

4) Employees should schedule bandwidth-intensive tasks like large file transfers, video downloads, mass e-mailing etc. for off-peak times.

Inappropriate Use

The following activities are prohibited on organization's Internet network. This list can be modified/updated anytime by the Management Committee as deemed fit. Any disciplinary action considered appropriate by the Management Committee (including legal action or termination) can be taken against an employee involved in the activities mentioned below:

1) Playing online games, downloading and/or watching games, videos or entertainment software or engaging in any online activity which compromises the network speed and consumes unnecessary Internet bandwidth

2) Downloading images, videos and documents unless required to official work

3) Accessing, displaying, uploading, downloading, storing, recording or distributing any kind of pornographic or sexually explicit material unless explicitly required for office work

4) Accessing pirated software, tools or data using the official network or systems

5) Uploading or distributing software, documents or any other material owned by the organization online without the explicit permission of the Management Committee

6) Engaging in any criminal or illegal activity or violating law

7) Invading privacy of coworkers

8) Using the Internet for personal financial gain or for conducting personal business

9) Deliberately engaging in an online activity which hampers the safety & security of the data, equipment and people involved.

10) Carrying out any objectionable, frivolous or illegal activity on the Internet that shall damage the organization's reputation

Information Security Policy

Objective Information security means protection of the organization's data, applications, networks and computer systems from unauthorized access, alteration and destruction. The Information Security Policy provides guidelines to protect data integrity based on data classification and secure the organization's information systems.

General Guidelines

1. Various methods like access control, authentication, monitoring and review will be used to ensure data security in the organization.

2. Security reviews of servers, firewalls, routers and monitoring systems must be conducted on a regular basis. These reviews should include monitoring of access logs and intrusion detection software logs.

3. Appropriate training must be provided to data owners, data users, and network & system administrators to ensure data security.

Data Classification

1. The organization classifies data into three categories:

a. High Risk: i. It includes information assets which have legal requirements for disclosure and financial penalties imposed for disclosure. ii. E.g. Payroll, personnel, financial, biometric data

b. Medium Risk: i. It includes confidential data which would not impose losses on the organization if disclosed, but is also not publicly available. ii. E.g. Agreement documents, unpublished reports, etc.

c. Low Risk: i. It includes information that can be freely disseminated. ii. E.g. brochures, published reports, other printed material etc.

2. Different protection strategies must be developed by the IT department for the above three data categories. Information about the same must be disseminated appropriately to all relevant departments and staff.

3. High risk data must be encrypted when transmitted over insecure channels.

4. All data must be backed up on a regular basis as per the rules defined by the IT Dept. at that time.

Email and Chat Policy

Objective

This policy provides information about acceptable usage, ownership, confidentiality and security while using electronic messaging systems and chat platforms provided or approved by the organization. The policy applies to all electronic messages sent or received via the above mentioned messaging systems and chat platforms by all official employees of the organization.

General Guidelines

1) The organization reserves the right to approve or disapprove which electronic messaging systems and chat platforms would be used for official purposes. It is strictly advised to use the pre-approved messaging systems and platforms for office use only.

2) An employee who, upon joining the organization, is provided with an official email address should use it for official purposes only.

3) Any email security breach must be notified to the IT Dept/Admin Dept immediately.

4) Upon termination, resignation or retirement from the organization, the organization will deny all access to electronic messaging platforms owned/provided by the organization.

5) All messages composed and/or sent using the pre-approved messaging systems and platforms need to comply with the company policies of acceptable communication.

6) Electronic mails and messages should be sent after careful consideration since they are inadequate in conveying the mood and context of the situation or sender and might be interpreted wrongly.

7) All email signatures must have appropriate designations of employees and must be in the format approved by the Management Committee.

Ownership

1) The official electronic messaging system used by the organization is the property of the organization and not the employee. All emails, chats and electronic messages stored, composed, sent and received by any employee or non-employee in the official electronic messaging systems are the property of the organization.

2) The organization reserves the right to intercept, monitor, read and disclose any messages stored, composed, sent or received using the official electronic messaging systems.

3) The organization reserves the right to alter, modify, re-route or block messages as deemed appropriate

4) IT Administrator/Admin Dept can change the email system password and monitor email usage of any employee for security purposes.

Confidentiality

1) Proprietary, confidential and sensitive information about the organization or its employees should not be exchanged via electronic messaging systems unless pre-approved by the Reporting Manager(s) and/or the Management Committee.

2) Caution and proper judgment should be used to decide whether to deliver a message in person, on phone or via email/electronic messaging systems.

3) Before composing or sending any message, it should be noted that electronic messages can be used as evidence in a court of law.

4) Unauthorized copying and distributing of copyrighted content of the organization is prohibited.

Email Security

1) Anti-Virus:

a. Anti-virus software pre-approved by the Dept. Head - IT should be installed in the laptop/desktop provided to a new employee after joining the organization.

b. All employees in the organization are expected to make sure they have anti-virus software installed in their laptops/desktops (personal or official) used for office work.

c. Organization will bear responsibility for providing, installing, updating and maintaining records for one anti-virus per employee at a time for the official laptop provided by the organization. The employee is responsible for installing good quality anti-virus software in their personal laptop/desktop used for office work.

d. Employees are prohibited from disabling the anti-virus software on organization provided laptops/desktops.

e. Employees should make sure their anti-virus is regularly updated and not out of date.

2) Safe Email Usage: Following precautions must be taken to maintain email security:

a. Do not to open emails and/or attachments from unknown or suspicious sources unless anticipated by you.

b. In case of doubts about emails/ attachments from known senders, confirm from them about the legitimacy of the email/attachment.

c. Use Email spam filters to filter out spam emails.

Inappropriate Use

1) Official Email platforms or electronic messaging systems including but not limited to chat platforms and instant messaging systems should not be used to send messages containing pornographic, defamatory, derogatory, sexual, racist, harassing or offensive material.

2) Official Email platforms or electronic messaging systems should not be used for personal work, personal gain or the promotion or publication of one's religious, social or political views.

3) Spam/ bulk/junk messages should not be forwarded or sent to anyone from the official email ID unless for an officially approved purpose.

Software Usage Policy

Objective

The Software Usage Policy is defined to provide guidelines for appropriate installation, usage and maintenance of software products installed in organization-owned computer

General Guidelines

1) Third-party software (free as well as purchased) required for day-to-day work will be preinstalled onto all company systems before handing them over to employees. A designated person in the IT Dept/Admin Dept can be contacted to add to/delete from the list of pre-installed software on organizational computers.

2) No other third-party software – free or licensed can be installed onto a computer system owned or provided to an employee by the organization, without prior approval of the IT Dept/Admin Dept

3) To request installation of software onto a personal computing device, an employee needs to send a written request via the IT Ticket System or IT Support Email.

4) Any software developed & copyrighted by the organization belongs to the organization. Any unauthorized use, storage, duplication or distribution of such software is illegal and subject to strict disciplinary action.

Compliance

1) No employee is allowed to install pirated software on official computing systems.

2) Software purchased by the organization or installed on organizational computer systems must be used within the terms of its license agreement.

3) Any duplication, illegal reproduction or unauthorized creation, use and distribution of licensed software within or outside the organization is strictly prohibited. Any such act will be subject to strict disciplinary action.

4) The Admin Dept. procedures & guidelines need to be followed to purchase new software (commercial or shareware) for official purposes. All approved software will be purchased through the Procurement Dept., unless informed/permitted otherwise.

5) Any employee who notices misuse or improper use of software within the organization must inform his/her Reporting Manager(s).

Software Audit

1) The IT /Admin Dept. will conduct periodic audit of software installed in all company-owned systems to make sure all compliances are being met.

2) Prior notice may or may not be provided by the IT Dept. before conducting the Software Audit.

3) During this audit, the IT /Admin Dept. will also make sure the anti-virus is updated, the system is scanned and cleaned and the computer is free of garbage data, viruses, worms or other harmful programmatic codes

4) The full cooperation of all employees is required during such audits